UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/260,796	03/01/1999	JAMES P HUGHES	98-019-NSC	6934

7590 08/26/2002

TIMOTHY R SCHULTE
STORAGE TECHNOLOGY CORPORATION
2270 SOUTH 88TH STREET MS-4309
LOUISVILLE, CO 800284309

EXAMINER
DARROW, JUSTIN T

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 08/26/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/260,796	Applicant(s) HUGHES, JAMES P	
	Examiner Justin T. Darrow	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 July 2002* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7,10,11,13 and 15-17* is/are rejected.

7)☒ Claim(s) *6,8,12 and 14* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 March 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-17 have been examined.

Response to Arguments

2. Applicant's arguments filed 07/01/2002 have been fully considered but they are not persuasive.

As per claims 1 and 2, Carter, U.S. Patent No. 5,787,175 A, points out that a user identifier and password is asked from a user requesting access to a work group document (see column 8, lines 51-59; figure 2, item 48; column 16, lines 16-29; figure 4, item 90; figure 9, step 152). Carter does not explicitly disclose the feature of an access formula. However, this feature is deemed to be inherent to the Carter method because the entered password would have to be compared with a stored value in order to determine granting user access (see column 16, lines 16-29; figure 4, item 90; figure 9, step 152). The Carter method would be inoperative if such a comparison were not made. Such a matching comparison is within the scope of an access formula as described by the applicant in the specification (see specification, page 10, lines 10-25 and figure 1, items 22 and 44). Therefore, Carter anticipates each element of claims 1 and 2 and these rejections are maintained.

As per claims 9-11, 13, and 15-17, Carter describes a system for the secure handling of information comprising: a generator of public-key cryptographic keys which corresponds to the recited key manager (see column 8, lines 60-65; column 11, lines 55-67; and figure 3, item 74, 76, 78, and 80); an object database system with group objects and key objects which corresponds to the claimed at least one group server (see column 10, lines 14-20 and figure 3, items 70 and

74); a collaborative access controller which corresponds to the recited at least one producer client encrypting the data portion of a document which corresponds to the recited data set with a randomly generated document key which corresponds to the claimed encryption value (see column 13, lines 4-17; figure 2, item 50 and 54; figure 4, item 94; and figure 6, step 112); arranging collaborative group identification by identifying a group object or other group identifier (see column 13, lines 18-28; figure 2, item 48; figure 3, item 70; and figure 6, step 114); encrypting the document key with the public key of the collaborative group (see column 13, lines 63-67; column 14, lines 1-5 and figure 5, item 100); including the member group definition and an encrypted message digest containing the encrypted document key in the work group document (see column 12, lines 25-55; figure 4, items 54, 90, 94, and 96; and figure 5, items 96, 98, 100, and 102); and storing the work group document in a file in a computer system (see column 12, lines 9-14 and figure 1, item 10). Carter does not explicitly disclose the feature of an access formula. However, this feature is deemed to be inherent to the Carter method because the entered password would have to be compared with a stored value in order to determine granting user access (see column 16, lines 16-29; figure 4, item 90; figure 9, step 152). The Carter method would be inoperative if such a comparison were not made. Such a matching comparison is within the scope of an access formula as described by the applicant in the specification (see specification, page 10, lines 10-25 and figure 1, items 22 and 44). Therefore, Carter anticipates each element of claim 9 and this rejection is maintained as well as those for claims 10, 11, 13, and 15-17.

As per claim 3, arranging collaborative group identification corresponds to the recited determining an access formula expressing logical combination of the at least one group for which

access to the information set will be granted, solution of the access formula by at least one solution group indicating that a consumer client belonging to the at least one solution group may access the encrypted information set. Carter points out authentication of collaborative group by obtaining user identifiers (see column 13, lines 18-28; figure 2, item 48; figure 3, items 68 and 70; and figure 6, item 114) which undergo validation (see column 13, lines 29-38) so that a group member or members can obtain the encrypted document key for accessing a document (see column 13, lines 63-67 and column 14, lines 1-5). Carter does not explicitly disclose the feature of an access formula. However, this feature is deemed to be inherent to the Carter method because the entered password would have to be compared with a stored value in order to determine granting user access (see column 13, lines 18-38). The Carter method would be inoperative if such a comparison were not made. Such a matching comparison is within the scope of an access formula as described by the applicant in the specification (see specification, page 10, lines 10-25 and figure 1, items 22 and 44). The applicant is incorrect that the passage of column 13, lines 18-28 refers to the forming of a group of members because such a group has already been formed. Therefore, the rejections of claims 3-5 and 7 are maintained.

Drawings

3. The drawings filed on 03/01/1999 are acceptable to the examiner and the draftperson.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) do not apply to the examination of this application as the application being examined was not (1) filed on or after November 29, 2000, or (2) voluntarily published under 35 U.S.C. 122(b). Therefore, this application is examined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

5. Claims 1, 2, 9, 11, 13, and 15-17 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by Carter, U.S. Patent No. 5,787,175 A.

As per claim 1, Carter illustrates a method for secure handling of information comprising: authenticating a user group with a user group identifier and corresponding password (see column 8, lines 51-59; figure 2, item 48; column 16, lines 16-29; and figure 9, step 152); as a result of authentication, obtaining the private key of the user (see column 16, lines 30-37 and figure 9, step 154); and using the private key to decrypt the encrypted document key that is required to decrypt the document (see column 16, lines 60-65 and figure 9, step 160).). Carter does not explicitly disclose the feature of an access formula. However, this feature is deemed to be inherent to the Carter method because the entered password would have to be compared with a stored value in order to determine granting user access (see column 16, lines 16-29; figure 4, item 90; figure 9, step 152). The Carter method would be inoperative if such a comparison were not made

As per claim 2, Carter embodies the functions of the operating system being incorporated in individual application programs to access documents (see column 9, lines 62-67; column 10, lines 1-2; figure 2, items 46, 48, 50, and 54; and figure 6, step 120).

As per claim 9, Carter describes a system for the secure handling of information comprising: a generator of public-key cryptographic keys which corresponds to the recited key manager (see column 8, lines 60-65; column 11, lines 55-67; and figure 3, item 74, 76, 78, and 80); an object database system with group objects and key objects which corresponds to the claimed at least one group server (see column 10, lines 14-20 and figure 3, items 70 and 74); a collaborative access controller which corresponds to the recited at least one producer client encrypting the data portion of a document which corresponds to the recited data set with a randomly generated document key which corresponds to the claimed encryption value (see column 13, lines 4-17; figure 2, item 50 and 54; figure 4, item 94; and figure 6, step 112); arranging collaborative group identification by identifying a group object or other group identifier (see column 13, lines 18-28; figure 2, item 48; figure 3, item 70; and figure 6, step 114); encrypting the document key with the public key of the collaborative group (see column 13, lines 63-67; column 14, lines 1-5 and figure 5, item 100); including the member group definition and an encrypted message digest containing the encrypted document key in the work group document (see column 12, lines 25-55; figure 4, items 54, 90, 94, and 96; and figure 5, items 96, 98, 100, and 102); and storing the work group document in a file in a computer system (see column 12, lines 9-14 and figure 1, item 10). As per claim 11, Carter points out that the member is verified if the corresponding identifier is found (see column 16, lines 51-62; column 15, lines 46-48; figure 5, item 98; and figure 9, step 154). Carter does not explicitly disclose the

feature of a boolean combination resultant of true. However, this feature is deemed to be inherent to the system of Carter as the finding of the member identifier in a logical alternative for access (see column 16, lines 51-62; column 15, lines 46-48; figure 5, item 98; and figure 9, step 154). The system of Carter would be inoperative if this logical consequence did not result. Carter does not explicitly disclose the feature of an access formula. However, this feature is deemed to be inherent to the Carter method because the entered password would have to be compared with a stored value in order to determine granting user access (see column 16, lines 16-29; figure 4, item 90; figure 9, step 152). The Carter method would be inoperative if such a comparison were not made.

As per claim 13, Carter additionally show obtaining the private key (see column 16, lines 30-33; figure 9, step 154); determining that the document to which access is requested is a work group document (see column 16, lines 16-19; figure 2, item 54; and figure 4, item 90); searching the collaborative document for the member identifier (see column 16, lines 51-55 and figure 9, step 158); request access to the work group document (see column 16, lines 16-19 and figure 4, item 90); using the private key to decrypt the corresponding encrypted document key (see column 16, lines 60-65 and figure 9, step 160); and using the document key to decrypt the encrypted data portion of the collaborative document (see column 17, lines 5-10; figure 4, items 90 and 94; and figure 9, step 162).

As per claim 15, Carter further elaborates a user requesting the addition of a new member (see column 14, lines 44-51); verifying this user (see column 14, lines 44-51 and figure 7, step 122); decrypting the encrypted document key with the private key (see column 15, lines 17-23;

figure 3, item 80; and figure 4, item 100); and encrypting the document key with the public key of the new member (see column 15, lines 22-23; figure 3, item 78; and figure 4, item 100).

As per claim 16, Carter suggests that the attempt to access the document is logged (see column 16, lines 44-50).

As per claim 17, Carter embodies the collaborative access controller operable to make changes including additions (see column 14, lines 44-51) and deletions (see column 15, lines 31-40).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 3-5 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carter, U.S. Patent No. 5,787,175 A in view of Feistel, U.S. Patent No. 3,798,360 A.

As per claim 3, Carter depicts a method for secure handling of information comprising: creating group objects (see column 10, lines 14-20 and figure 3, item 70); obtaining a public key and private key (see column 11, lines 61-67; column 12, lines 1-8; and figure 3, items 76, 78, and 80); encrypting the data portion of a document with a generated document key, preferably for use with a symmetric encryption method (see column 13, lines 4-17; figure 2, item 50 and 54; figure 3, items 68 and 70; figure 4, item 94; and figure 6, step 112); authentication of collaborative

group by obtaining user identifiers (see column 13, lines 18-28; figure 2, item 48; and figure 6, item 114) which undergo validation (see column 13, lines 29-38) so that a group member or members can obtain the encrypted document key for accessing a document (see column 13, lines 63-67 and column 14, lines 1-5); encrypting the document key with the public key of the collaborative group (see column 13, lines 63-67; column 14, lines 1-5 and figure 5, item 100); including the member group definition containing the encrypted document key in the work group document (see column 12, lines 25-42; figure 4, items 54, 90, 94, and 96; and figure 5, item 100); and storing the work group document in a file in a computer system (see column 12, lines 9-14 and figure 1, item 10). Although Carter describes that the document key is preferably suitable for use with a symmetric cryptographic method (see column 13, lines 7-10), he does not explicitly teach that it is randomly generated. Feistel specifies a random key number generator in a symmetric key block cipher (see column 5, lines 18-23 and figure 1, item 43). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the method for the secure handling of information of Carter with the random key generator of Feistel to have a degree of security that relates to the probability of guessing the unique combination of key binary digits by an opponent having both the knowledge of the internal circuitry of the system and the opportunity to observe prior transmissions and resulting ciphers (see column 5, lines 9-14).

As per claim 4, Carter further elaborates a user requesting the addition of a new member (see column 14, lines 44-51); verifying this user (see column 14, lines 44-51 and figure 7, step 122); decrypting the encrypted document key with the private key (see column 15, lines 17-23;

figure 3, item 80; and figure 4, item 100); and encrypting the document key with the public key of the new member (see column 15, lines 22-23; figure 3, item 78; and figure 4, item 100).

As per claim 5, Carter suggests that the attempt to access the document is logged (see column 16, lines 44-50).

As per claim 7, Carter points out that the member is verified if the corresponding identifier is found (see column 16, lines 51-62; column 15, lines 46-48; figure 5, item 98; and figure 9, step 154). Carter does not explicitly disclose the feature of a boolean combination resultant of true. However, this feature is deemed to be inherent to the method of Carter as the finding of the member identifier in a logical alternative for access (see column 16, lines 51-62; column 15, lines 46-48; figure 5, item 98; and figure 9, step 154). The method of Carter would be inoperative if this logical consequence did not result.

8. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Carter, U.S. Patent No. 5,787,175 A in view of as applied to claim 9 above, and further in view of Feistel, U.S. Patent No. 3,798,360 A.

Carter discloses the system for the secure handling of information of claim 9. Although Carter describes that the document key is preferably suitable for use with a symmetric cryptographic method (see column 13, lines 7-10), he does not explicitly teach that it is randomly generated. Feistel specifies a random key number generator in a symmetric key block cipher (see column 5, lines 18-23 and figure 1, item 43). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the system for the secure handling of information of Carter with the random key generator of Feistel to have a degree of security that relates to the probability of guessing the unique combination of key

binary digits by an opponent having both the knowledge of the internal circuitry of the system and the opportunity to observe prior transmissions and resulting ciphers (see column 5, lines 9-14).

Allowable Subject Matter

9. Claims 6, 8, 12, and 14 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

10. The following is a statement of reasons for the indication of allowable subject matter: Claims 6 and 14 are drawn to a method and system for the secure handling of information, respectively. The closest prior art, Carter, U.S. Patent No. 5,787,175 A, discloses a similar method and system. However, he neither teaches nor suggests an encrypted partial key for each group in a plurality of groups, encrypted with the public key for that group, and each partial key required to decrypt the encrypted randomly generated number. This combination of limitations explicitly incorporated in dependent claims 6 and 14 renders them to have allowable subject matter. Claims 8 and 12 are drawn to a method and system for the secure handling of information, respectively. The closest prior art, Carter, U.S. Patent No. 5,787,175 A, discloses a similar method and system. However, he neither shows nor motivates prohibiting storage on the at least one trusted storage device in the information set is determined not to be encrypted. This step explicitly recited in dependent claims 8 and 12 renders them to have allowable subject matter.

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (703) 305-3872 and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (703) 305-1830.

The fax numbers for Formal or Official faxes to Technology Center 2100 are (703) 305-0040 and (703) 746-7239. Draft or Informal faxes for this Art Unit can also be submitted to (703) 746-7240. In order for a formal paper transmitted by fax to be entered into the application

file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to (703) 746-7238 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-3900.

Justin Darrow

Justin T. Darrow

Patent Examiner

Technology Center 2100

August 22, 2002